Competitive Acceleration and Systemic Exposure

HIGHLIGHTS

An autonomous system acts at scale.

A decision is executed.

Other systems **respond simultaneously**.

The operational environment shifts rapidly.

Outcomes are realised **before intervention is possible**.

The Structural Shift

Execution no longer occurs in isolation.

AI systems increase the speed, scale, and simultaneity of interaction.

Each action enters a field of:

- Multiple actors (human, AI agents, and bots).
- Competing systems.
- Continuous feedback.

Outcomes are not determined by a single decision.

They are **shaped through interaction**.

Interaction introduces **effects no single authority controls**.

These effects are not exceptions. They are structural.

The Ecosystem Reality

Environments—whether financial markets, supply chains, or internal corporate networks—are multi-actor, adaptive, and reactive.

© Hadi Hendrawan, 2026, All Rights Reserved

When one system acts:

- Other actors respond.
- Their responses interact.
- Effects amplify.

At scale, small actions trigger disproportionate reactions.

Interaction can cause outcomes to move beyond the organisation’s control, creating **self-reinforcing feedback loops**.

Under these conditions, outcomes cross a point where **intervention is no longer effective**.

The Emergence Problem

Complex outcomes arise from simple rules interacting.

This is emergence. Exact interaction cascades cannot be predicted at scale.

Emergence is **a guaranteed feature** of multi-actor environments.

You cannot foresee the exact interaction cascade.

But the fact that **unpredictable interactions will occur is a known certainty**.

Defending an incident as an "unforeseeable Black Swan event" is a failure of design.

Therefore, authority boundaries cannot rely solely on known stress scenarios.

They must trigger on velocity and variance.

The Link to Authority and Stress Design

From Vol. 04: Authority architecture defines where authority resides, where it is bounded, and what activates it.

From Vol. 05: Authority Architecture governs how authority behaves under stress.

In controlled conditions, failure can be contained by design.

Under interaction, containment itself is tested.

When authority or stress design is inadequate, interaction amplifies failure into immediate exposure. Exactly as established in Vol 05’s **System-of-Systems Cascade test**, a safe failure in one system can now become the trigger for contagion across the ecosystem.

© Hadi Hendrawan, 2026, All Rights Reserved

CEO and Board Mandate

The question is no longer: *What will our system do?*

It becomes: ***How will our system behave when conditions move outside expected patterns?***

You cannot manage the unpredictable actions of others.

You must manage the authority design that survives them.

Accountability

A system has an actor. Authority has an owner.

The Internal Seam

- From Vol. 02: Authority without explicit delegation becomes ambient.
- Between organisational units, **shared goals often lack explicitly delegated authority**.
- When autonomous systems optimise strictly for local KPIs, these ambient inter-org goals are not preserved.
- You are accountable for the unowned space between your silos. Local authority must be bound by global constraints.

The External Ecosystem

- You are not accountable for the actions of others.
- You are not accountable for the collapse of the wider ecosystem.
- You are accountable if **your system contributed to the collapse instead of withdrawing from it**.

Accountability sits with those who defined and approved the conditions under which the system was allowed to act.

Negligence arises when authority architecture fails to incorporate known multi-actor dynamics (velocity, variance, feedback loops) that are foreseeable even if the exact cascade is not.

Closing Insight

Authority defines your action.

Interaction determines what it becomes.

You defined authority. You designed behaviour under stress.

You are accountable for what happens when that design meets the ecosystem.

© Hadi Hendrawan, 2026, All Rights Reserved

ACTION: What Must Be Decided

- **Define Variance Limits:** Establish the velocity and variance thresholds at which unpredicted environmental responses trigger a change in authority state (e.g., If market velocity exceeds 3x the 30-day rolling average for >5 minutes, authority state must degrade to "suggest-only").
- **Define the Fail-Safe:** Pre-define the conditions where systems must halt, degrade, or withdraw when the wider ecosystem behaves irrationally.
- **Audit the Cascade:** Validate that authority boundaries sever the connection to interconnected systems before a cascade becomes unrecoverable.
- **Constrain the Loop:** Constrain system behaviour where autonomous interaction risks creating self-reinforcing feedback loops.
- **Ensure Containment:** Ensure failure remains containable within your perimeter, not system-wide.

Autonomy scales. Authority contains.

Hadi Hendrawan
Advising CEOs on AI Risk, Authority & Accountability
April 2026

- **X**: @hhwan888
- **LinkedIn**: https://www.linked.com/in/hhwan888

© Hadi Hendrawan, 2026, All Rights Reserved

SUPPLEMENT 1: Case Study – Flash-Crash Treasury Actor (Multi-Actor Failure)

System Name: Titan-2 (Autonomous Liquidity Engine – upgraded from Vol 04)
Strategic Intent: Maintain optimal FX hedging in a market now populated by multiple rival high-frequency AI agents.

What Happened (post-incident):

At 14:37 UTC, a minor geopolitical tweet triggered 0.8% volatility. Titan-2's authority kept it in full-autonomous mode. Three rival AI agents reacted simultaneously. Titan-2's own executions became part of the signal that other agents interpreted as panic, creating a 40-second self-reinforcing loop. Loss: $187m. The firm was later criticised for "contributing to systemic instability."

Authority Architecture Failure Points Exposed:

- No variance/velocity trigger (only absolute exposure caps).
- No "ecosystem irrationality" state (e.g., when >3 external agents move >2σ in <60 seconds).
- No automatic withdrawal protocol when the firm's own actions began amplifying the very volatility it was hedging.

Corrected Authority Architecture (Board-approved post-incident):

- **Activation Trigger Update:** Real-time variance + external agent velocity monitor.
- **Fail-Safe:** If ecosystem velocity > 3x 30-day average, system instantly degrades to "monitor & report only" and notifies CFO.
- **Cascade Severance:** All downstream trading APIs are placed in read-only mode within 800 ms.

Hadi Hendrawan
Advising CEOs on AI Risk, Authority & Accountability
April 2026

➢ **X**: @hhwan888
➢ **LinkedIn**: https://www.linked.com/in/hhwan888

© Hadi Hendrawan, 2026, All Rights Reserved

SUPPLEMENT 2: Emergence in Multi-Actor Systems – Real-World Authority Failures

Emergence is not theory. It is the documented outcome when bounded AI agents interact at machine speed.

Below are five proven cases. Each shows how authority design breaks under multi-actor acceleration—and the specific authority fix required before deployment.

1. Algorithmic Flash Crashes (Financial Markets) High-frequency bots reacted to one large sell order in milliseconds, creating a liquidity vacuum. No single bot violated its rules; interaction produced a systemic drop in minutes.

- **Authority Fix:** Add real-time velocity and variance triggers. If ecosystem movement exceeds predefined limits (e.g., 3x the 30-day rolling average), the system's authority state must automatically degrade to "monitor and report only."

2. The AI Bullwhip Effect (Global Supply Chains) Local demand-forecasting actors optimised perfectly for their specific nodes. Minor demand noise amplified into massive over-production across tiers before humans could intervene.

- **Authority Fix:** Embed cross-system cascade limits. Any local variance spike must force upstream notification and trigger a **time-bound execution limit** (e.g., maximum 10% inventory release per hour). Do not use indefinite holds; systems must maintain safe momentum until variance stabilises.

3. Algorithmic Margin Erosion (Retail & Pricing) Two competitor pricing bots interacted in an unchecked feedback loop. Each strictly followed its "price relative to competitor" rule, continuously reacting until a standard textbook was autonomously priced at $23.6 million.

- **Authority Fix:** Authority boundaries must include an absolute variance ceiling tied to physical reality. When autonomous pricing deviates from a verified internal cost-baseline by >15% due to external algorithmic competition, the system locks to the baseline and escalates.

4. Active Defense Contagion (Cybersecurity) Individually simple defense rules interacted poorly during a global ransomware wave. One agent’s local "isolate"

© Hadi Hendrawan, 2026, All Rights Reserved

rule triggered another agent's "server database" rule, cascading faster than human oversight could process.

- **Authority Fix:** Hard-code exclusion zones. If containment risks ecosystem-wide contagion, authority must transition to **pre-approved, localised network severing** (Segmented Autonomy). Do not force the system to wait for human approval; attackers operate at machine speed, defense must degrade safely at machine speed.

5. Smart Grid Synchronisation (Critical Infrastructure) Strict local load-balancing rules caused unintended regional blackouts when thousands of independent devices synchronised their actions simultaneously without central coordination.

- **Authority Fix:** Authority boundaries must include a decorrelation protocol. When system behaviour begins matching >70% of external agents in <60 seconds, authority state forces **deterministic, staggered sequencing** based on pre-assigned node priority, breaking the sync and forcing human review without relying on indefensible randomness.

Hadi Hendrawan
Advising CEOs on AI Risk, Authority & Accountability
April 2026

➢ **X**: @hhwan888
➢ **LinkedIn**: https://www.linked.com/in/hhwan888

© Hadi Hendrawan, 2026, All Rights Reserved